Piratenpartei Österreichs
www.piratenpartei.at

Geschäftszahl: BMVIT-630.333/0001-III/PT2/2009

Stellungnahme zu dem Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird

Zusammenfassung

Eine grundrechtskonforme Umsetzung der EU-Richtlinie 2006/24/EG ist nicht möglich - die einzige Alternative zu dem derzeitigen Entwurf ist daher die Nichtumsetzung. Ein Vertragsverletzungsverfahren kann riskiert werden, da solche Verfahren ausgesprochen trivial sind. Österreich ist durchaus regelmäßig mit solchen konfrontiert. Durch die Nichtumsetzung alleine entstehen der Republik keine Kosten.

Argumentation

Fehlender Schutz für Informanten und Klienten bestimmter Berufsgruppen

Es gibt Berufsgruppen, welche nicht ohne Grund, schon seit sehr langer Zeit der Verschwiegenheitspflicht unterliegen. Rechtsanwälte, Steuerberater, Notare und Wirtschaftstreuhänder würden sich durch die Preisgabe von Informationen vor den geltenden Gesetzen strafbar machen und liefen Gefahr, ihre Anstellung oder Zulassung zu verlieren. Sie würden das Vertrauen ihrer Kunden einbüßen, was nicht zuletzt schwere wirtschaftliche Konsequenzen hätte. Journalisten sind für eine umfassende Berichterstattung auf verlässliche Quellen angewiesen. Diese sind aber ihrerseits von der Sicherheit ihrer Daten abhängig und teilweise nur unter dieser Bedingung zu einer Kooperation bereit. Ärzte und vor allem Priester verpflichten sich darüber hinaus vor allem aus ethischen Gründen zur streng vertraulichen Behandlung persönlicher Daten und anderer Informationen. Es entspricht dem gesellschaftlichen Verständnis, dass alle oben genannten Berufsgruppen der Verschwiegenheit verpflichtet sind – niemand kann es sich anders vorstellen oder würde es sich anders wünschen. Ebenso unbestritten ist, dass verschiedene Behörden, einschließlich der Strafverfolgungsbehörden, mit vielerlei persönlichen Daten arbeiten und dass die Weitergabe von Informationen, in vielen Fällen nach Anordnung eines Gerichtes, zur Unterstützung von Ermittlungen jedenfalls zu erfolgen hat. Die Speicherung von Verbindungsdaten auf Vorrat und die daraus entstehende Nachvollziehbarkeit von Kontakten, Aktivitäten und Interessen kann jedoch die beruflichen Beziehungen zwischen Dienstleister und Kunden destabilisieren und dadurch unerwartete wirtschaftliche und gesellschaftliche Auswirkungen haben. Insbesondere der Journalismus wird in seinen Möglichkeiten stark eingeschränkt, und mit ihm automatisch die Pressefreiheit. Die Unabhängigkeit in der Berichterstattung ist ein Stützpfeiler jeder demokratischen Gesellschaft. Um diesen zu schützen, muss von der Umsetzung der Vorratsdatenspeicherung abgesehen werden.

Piratenpartei Österreichs
www.piratenpartei.at

Fehlende Auskunftspflicht für Betroffene

Ein weiterer, bedeutender Kritikpunkt ist, dass keine Informationspflicht nach dem Abrufen von Daten festgeschrieben ist. Es war demnach zu keiner Zeit vorgesehen, die Betroffenen von einer Amtshandlung, die so tief in ihren Persönlichkeitsbereich eindringt, in Kenntnis zu setzen. Eine einzige Einschränkung gibt es, welche aber an Ironie kaum zu überbieten ist: Im seltenen Fall, dass über ein Mobiltelefon ein Notruf abgesetzt wird, wird der Besitzer des Anschlusses benachrichtigt. Der Vorwurf der Überwachung bezieht sich zu einem großen Teil auf diese Problematik – solange man nicht sicher sein kann, dass man erfährt, wenn jemand auf seine persönlichen Daten zugegriffen hat, bleibt endlos viel Spielraum für Spekulationen, denn es könnte ja jederzeit passieren. Darüber hinaus gibt es keine Möglichkeit, im Zweifelsfall die Rechtmäßigkeit einer Abfrage zu überprüfen, da der Vorgang nicht kommuniziert wird. Wir sehen dies als weiteren Grund, die Nichtumsetzung der Richtlinie zu empfehlen.

Datenschutzkommission nicht unabhängig

Die gemäß Paragraph 102c Absatz 1 für die Kontrolle der Datenübergabe und der Datensicherheitsmaßnahmen zuständige Datenschutzkommission ist nicht weisungsfrei und unabhängig. Dies wurde auch schon von der EU-Kommission festgestellt und beanstandet, da Artikel 9 (2) der Richtlinie 2006/24/EG eine völlige Unabhängigkeit der Kontrollstelle verlangt (Vertragsverletzungsverfahren läuft).

Fehlende Wirtschaftlichkeit

Da kein Ersatz für zusätzliche Personalkosten der Provider vorgesehen ist, werden die Kosten der Datenspeicherung an die Kunden weiter verrechnet werden. Die Telekommunikationsanbieter unterhalten mittlerweile ganze Abteilungen, die sich nur um die Pflege der Vorratsdatenbanken und die Abfragen der Behörden kümmern. Selbst für international erfolgreiche Unternehmen sind das Aufwendungen, welche schmerzlich spürbar sind, zumal diese Abteilungen niemals Gewinn oder auch nur Umsatz erwirtschaften werden.

Auch die Folgen einer ggf. nicht unwahrscheinlichen Rückgängigmachung der Richtlinie zu einem späteren Zeitpunkt sollten beachtet werden. In verschiedenen Staaten laufen noch Verfahren, welche die Rechtmäßigkeit der Umsetzung prüfen. Die Summen, die von den Beteiligten bis zu diesem Moment aufgebracht wurden, wären schlecht investiert gewesen. Vor allem die betroffenen Telekommunikationsanbieter hätten hohe Verluste, die ihnen nicht ersetzt würden. Unter Umständen könnten berechtigte Schadensersatzansprüche entstehen. In Rumänien beispielsweise wird es keine Vorratsdatenspeicherung geben. Dort hat das Verfassungsgericht bereits befunden, dass diese mit der geltenden Verfassung nicht in Einklang zu bringen ist.

Auf der anderen Seite ist eine Nichtumsetzung seitens der Republik Österreich ohne größeres finanzielles Risiko. Damit es aufgrund eines Vertragsverletzungsverfahrens nach Artikeln 226 bzw. 228 EG-Vertrag zu Strafzahlungen kommt, ist ein entsprechendes Urteil des EUGh notwendig.

Piratenpartei Österreichs
www.piratenpartei.at

Verschlüsselung der Daten

Zwar wurde in §94 (4) die Verschlüsselung der Datenübertragung normiert, die Speicherung der Daten darf jedoch unverschlüsselt erfolgen. Eine verschlüsselte und dezentrale Datenhaltung wäre jedoch im Sinne des Zugriffsschutzes dringend geboten. Es ist klar, dass dadurch die Kosten für die Provider weiter erhöht werden. Wir machen daher auch hier auf die Möglichkeit der Nichtumsetzung aufmerksam.

Löschen der Daten

Die Paragraphen 99 (1) und 102a (8) normieren Löschpflichten. Was "Löschen" oder "Anonymisieren" im technischen Kontext bedeutet, wird jedoch offen gelassen. Die üblichen Löschverfahren in der IT stellen nicht sicher, dass auch technisch wenig versierte Personen oder einfach gehaltene Spionageprogramme die Daten nicht wieder herstellen können. Das Problem verschärft sich durch die Verpflichtung zur Datensicherheit und Protokollierung nach §102c. Dessen Anforderungen bedingen einerseits Backups und somit Redundanz, wodurch potentiell mehr Zugriffsmöglichkeiten entstehen. Andererseits verlangt er von den Providern die Implementierung von Schutzmaßnahmen. Praktisch bedeutet dies, dass Provider finanziell und personell aufstocken müssen. Personelle Aufstockung erfolgt in der IT meist temporär beziehungsweise anlassbezogen durch vermittelte unternehmensexterne Berater. Oft sind dem Unternehmen nicht mehr Informationen bekannt, als "das macht ein erfahrener Experte der Firma X zu den Kosten Y. Firma X bezieht den Experten aus einem der Z Staaten, in denen sie vertreten ist". Somit sind mehr und dem Unternehmen weniger bekannte Personen dafür zuständig, den Zugriff auf wenige Personen zu beschränken, wofür sie jedoch selbst Zugriff auf sämtliche Daten haben. Es kann daher angenommen werden, dass in den Regelungen ein Zielkonflikt besteht, der das Missbrauchspotential erhöht. Die Lösung des Konflikts sehen wir in der Nichtumsetzung der Richtlinie.

Mangelhafter Zugriffsschutz

Die Auswertung der Daten kann nur durch Spezialisten erfolgen. Durch die notwendigen Vorkenntnisse für den effizienten Umgang mit Verkehrs- und Verbindungsdaten wird dieser in die Hände einer bestimmten Berufssparte gelegt. Diejenigen Personen, die über das notwendige Fachwissen verfügen, werden teilweise nicht klassisch angestellt, sondern arbeiten oft auf Werkvertragsbasis und bleiben damit arbeitsrechtlich unabhängig. Sie können zugleich für Konzerne, Geheimdienste oder Terroristen arbeiten, es wird nicht zwingend nachvollziehbar sein. Die Strafverfolgung wird auf diese Weise privatisiert, da nicht mehr ausschließlich Organe der Behörden darin involviert sind. Zudem sind die Daten für weitaus mehr Personen zugänglich, als im Sinne einer engen Regelung vorgesehen wäre. Da die rechtlich vorgesehene Einschränkung der Zugriffsberechtigung praktisch nicht gewährleistet ist und es keinen Überblick darüber gibt, welche Personenkreise Zugang zu den Datenbanken der Telekommunikationsanbieter haben, herrscht diesbezüglich eine große Unsicherheit. Unter diesen Umständen ist eine Nichtumsetzung nahe zu legen.

Vgl. EKIS Skandale: Das Elektronische Kriminalpolizeiliche Informationssystem (EKIS) ist eine Zusammenfassung von elf Datenbanken des österreichischen Innenministeriums. Im EKIS enthalten sind unter anderem die zentrale Wählerevidenz, das Waffenregister, Kfz-Zulassungen, Strafregister sowie Personen-, Sachen- und Kulturgutfahndung sowie die DNA-Datenbank. In den vergangenen Jahrzehnten ist das EKIS regelmäßig im Zentrum von Datenmissbrauchsskandalen gestanden, zuletzt in der sogenannten Spitzelaffäre.

Fehlende Treffsicherheit

Die umzusetzende EU-Richtlinie wurde als wettbewerbsrechtliche Regelung mit Bezügen auf die Bekämpfung schwerer Verbrechen beschlossen (siehe die Begründung des EUGh im Verfahren gegen Irland C-301/06). Doch stellt sich die berechtigte Frage: Wie soll damit Terrorismus bekämpft werden? Es wird zwar der Großteil der Bevölkerung pauschal überwacht, einzelne Schwerkriminelle können jedoch ausweichen. Kleine Provider und Telekommunikationsanbieter können sich die Vorratsdatenspeicherung nicht leisten. Sie sind zwar aus diesem Grund von der Richtlinie ausgenommen, jedoch macht ohne sie eine Überwachung zum Zweck der Bekämpfung der Schwerkriminalität keinen Sinn. Darüber hinaus haben kleinere Unternehmen im Kommunikationsbereich durch die verpflichtenden hohen Aufwendungen für große Anbieter einen nicht zu vernachlässigenden Wettbewerbsvorteil gewonnen. So betrachtet läuft die Vorratsdatenspeicherung entschieden an ihrer Zielsetzung vorbei.

Erweiterte Problemstellung

Aus der EU-Richtlinie zur Vorratsdatenspeicherung erwachsen über die oben formulierten Schwierigkeiten hinaus noch einige andere Probleme, auf die hier auch kurz eingegangen werden soll.

IPv6 und eine ungewisse Zukunft

Die Umsetzung der Richtlinie sieht derzeit vor, fest vergebene und dynamisch vergebene IP-Adressen zu unterscheiden. Fest vergebene IP-Adressen werden in der Erweiterung des §92 Abs. 3 als Stammdaten normiert, dynamische IP-Adressen als Verkehrsdaten. Sowohl durch den Entwurf zur Umsetzung der Vorratsdatenspeicherung als auch durch das OGH Urteil vom 14.7.2009, 4 Ob 41/09x, erfahren dynamische IP-Adressen höheren Schutz als Stammdaten. Durch die kommende Umstellung der Adressräume auf IPv6 (RFC 2460) werden dynamisch vergebene IP-Adressen jedoch hinfällig. Weiters existieren neben öffentlichen dynamischen IP-Adressen, die von der Vorratsdatenspeicherung erfasst sind, auch private Adressräume, die von der Vorratsdatenspeicherung aus verständlichen Gründen nicht betroffen sind. Auch hier könnte es, zumindest langfristig, zu einer Entwicklung hin zu öffentlichen Adressräumen kommen. Die Zukunft wird eine explosionsartige Vermehrung an Geräten bringen, die über das Internet kommunizieren. Im Bereich mobiler Geräte ist der Trend bereits offensichtlich. Welche weiteren Geräte in Zukunft mit dem Internet verbunden sein werden, hat sich noch nicht konkretisiert. Es gibt jedoch bereits zahlreiche Konzepte, die allesamt zu einer drastischen Vermehrung des Datenaufkommens führen werden.

Piratenpartei Österreichs
www.piratenpartei.at

Erstellung von Persönlichkeitsprofilen

Überwachung ist bereits jetzt großflächig und vernetzt. Handlungsmuster und Gewohnheiten sind ohne großen Aufwand erkennbar. Vor allem das Internet ist eine aufschlussreiche Quelle, wenn es um die persönlichen Interessen und Kontakte von Einzelpersonen geht. Im Zusammenhang damit muss erwähnt werden, dass hier eine der wenigen Einschränkungen der Vorratsdatenspeicherung ausgehebelt wird, da die jeweiligen Inhalte im Fall von Webseiten und anderen Online-Medien leicht ersichtlich sind. Ein nicht unbedeutender Teil der Kommunikation und Informationsbeschaffung spielt sich heutzutage im Internet ab. Durch die Speicherung aller Zugriffe auf Webseiten und der zugehörigen IP-Adressen wird offen gelegt, wer wann welche Inhalte aufgerufen hat. Durch Zusammenführung dieser Daten mit den Bewegungsprofilen, deren Erstellung durch die Standortfeststellung von Mobiltelefonen, die Videoüberwachung im öffentlichen Raum und die Kennzeichenerkennung möglich ist, entsteht schon ein grobes Persönlichkeitsprofil. Ergänzt durch Verbindungsdaten hat man schon einen ziemlich genauen Überblick über die sozialen Kontakte und damit über das Leben einer beliebigen Person. Es besteht die theoretische Möglichkeit, Abweichungen von der Norm wahrzunehmen und zu vermerken. Für die Bürger entsteht ein Klima der ständigen Überwachung und Kontrolle. In diesem Klima ist die Weiterentwicklung der Bürgergesellschaft nicht mehr möglich.

Gefahr der Wirtschaftsspionage

In vergleichbarer Art können so Planungs- und Entwicklungsvorgänge innerhalb fortschrittlicher Unternehmen analysiert und antizipiert werden, was dem Tatbestand der Wirtschafts- oder Industriespionage nahe käme.

Missbrauch

Die missbräuchliche Nutzung der vorhandenen Daten ist, wie oben bereits erwähnt, äußerst wahrscheinlich. Aufgrund der hohen Anzahl von zugriffsberechtigten Personen und der fehlenden Kontrolle bleibt die einzelne Anfrage anonym und hinsichtlich ihrer Berechtigung meist ungeprüft. Die Ereignisse rund um eine weitere Datensammlung, das EKIS, zeigen sehr deutlich, wie mit sensiblen Informationen umgegangen werden kann und wird.

Weitere Begehrlichkeiten

Seit Beginn der Diskussion um die Vorratsdatenspeicherung bestehen bereits Begehrlichkeiten anderer Bereiche, beispielsweise Rechteverwerter und Verlagswesen, auf die gesammelten Daten zur Verfolgung eigener Ziele zuzugreifen. Auch für private Ermittler und Sicherheitsunternehmen wäre diese Möglichkeit äußerst interessant. Es ist nur eine Frage der Zeit, bis gezieltes Lobbying erste Früchte trägt und der ohnehin große Kreis der zugriffsberechtigten Personen erneut erweitert wird. Die Folge wäre die Verfolgung von Bagatelldelikten auf Basis der Auswertung von vorrätig gespeicherten Daten, was eindeutig nicht vorgesehen ist.

Piratenpartei Österreichs
www.piratenpartei.at

INDECT

Die EU-Richtlinie 2006/24/EG ist nach der Überarbeitung des DSG im Jahr 1999, der Überwachungsverordnung aus dem Jahr 2002, der Anpassungen im SPG im Jänner 2008, und anderen kleineren Punkten nicht mehr, als ein weiterer Schritt zur großflächigen Umsetzung von INDECT. Dieses hoch dotierte EU-Projekt, welches sich als „Intelligentes Informationssystem, das für die Sicherheit von Bürgern in einer städtischen Umgebung Überwachung, Suche und Entdeckung unterstützt“ (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) betitelt, gilt nicht zu unrecht als universelles Überwachungsinstrument, welches alle bereits bestehenden Überwachungstechnologien zentralisieren und automatisieren kann: Videoüberwachung samt Gesichtserkennung ist in Zeiten biometrischer Reisepässe und Personalausweise ein Kinderspiel; die Aufenthaltsbestimmung per GPS oder Standortsabfrage beim Telekommunikationsanbieter sowie die Verfolgung aller zurückgelegten Wege technisch keine Herausforderung. Mit der Vorratsdatenspeicherung eröffnet sich nunmehr die Möglichkeit zur Nachvollziehung sozialer Gefüge, da jeder Kontakt einer Person mit einer anderen – per Telefon, Handy oder Internet; in mündlicher oder schriftlicher Form – aufgezeichnet wird. Gepaart mit dem aktuell diskutierten Transferkonto für Sozialleistungen, welches die sensibelsten, nämlich die finanziellen und sozialen Informationen über alle Einwohner bündelt, ist mit einem „Klick“ das ganze Leben jedes beliebigen Menschen abrufbar.

Die Piratenpartei Österreichs warnt an dieser Stelle eindringlichst vor den absehbaren Entwicklungen und fordert die Österreichische Bundesregierung dazu auf, die EU-Richtlinie zur Vorratsdatenspeicherung nicht umzusetzen!

Für den Bundesvorstand:

Harald Haas, Max Lalouschek, Peter Stadlmaier